認知不足的風險

安達保險香港
2019年中小企網絡安全就緒度調查報告

CHUBB®

目錄

引言

Mr Andrew Taylor,
安達亞太區網絡保險保險產品負責人，
泰思博

2018年，安達保險首次針對香港特別行政區(香港)中小企展開網絡安全就緒度調查。今年，我們欣然發佈香港中小企網絡安全就緒度調查報告(第二版)。

作為全球最大的網絡保險公司之一，我們認為本報告對提高中小企業對管理網絡風險的認識非常重要。據預測，未來幾年，網絡風險將導致全球企業蒙受重大的收入損失。鑑於中小企業佔全港企業總數的98%，倘若未能在風險紓緩措施、緊急應變計劃及購買網絡保險方面做足準備，中小企業將遭受重大衝擊。[1]

2019年，四分之三(76%)的受訪中小企業表示曾遭遇網絡事故，儘管有上升趨勢，但在發生網絡事故後，逾三分之一(34%)的中小企業雖然會檢討保安措施，卻並無採取進一步行動，僅有11%的企業嘗試修復遭破壞的資料檔案。而近半數(47%)中小企領導者表示，僱員並未意識到企業所面臨網絡風險的嚴重性。由於僱員通常是網絡防禦的第一道亦是最佳的防線，而這重要的一點卻常被忽略。

我們希望本報告提供有用的卓見，幫助香港中小企業減低網絡風險。

[1] http://multimedia.scmp.com/native/infographics/article/3005155/sme-growth-guide/

認知不足的風險

網絡風險概況

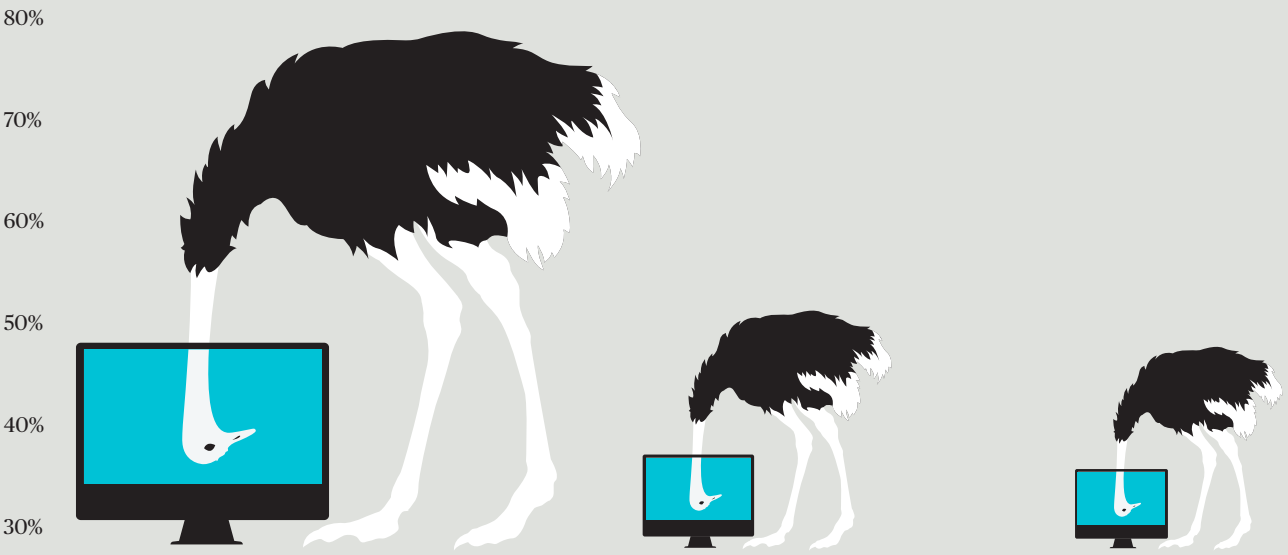
2018年，香港發生逾9,000宗網絡攻擊事故，導致企業損失22億港元。

香港已推出網絡防衛評估框架（「評估框架」），以提升金融業的資訊保安水平。[2]

互聯網經濟

香港的互聯網經濟迅速發展，預計於2022年將達58億美元。[3]

調查結果摘要



76%

去年，76%香港的中小企業曾遭遇網絡事故

47%

47%香港的中小企業領導者表示，僱員並未認識到企業面臨的網絡風險的嚴重性。

45%

45%香港的中小企業並未完全了解相關保險解決方案及保險在網絡風險管理方面所發揮的作用。

[2] https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf

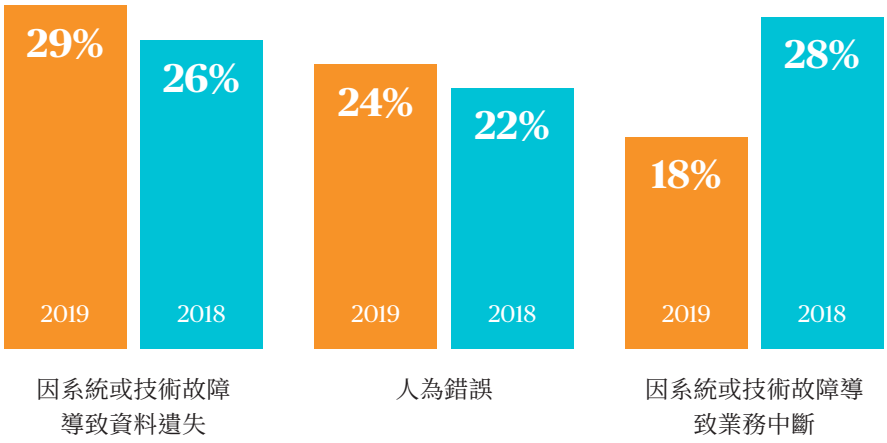
[3] https://www.scmp.com/business/companies/article/2149582/hong-Kong SARs-digital-spending-surge-us58b-2022-consumers-turn

風險無處不在

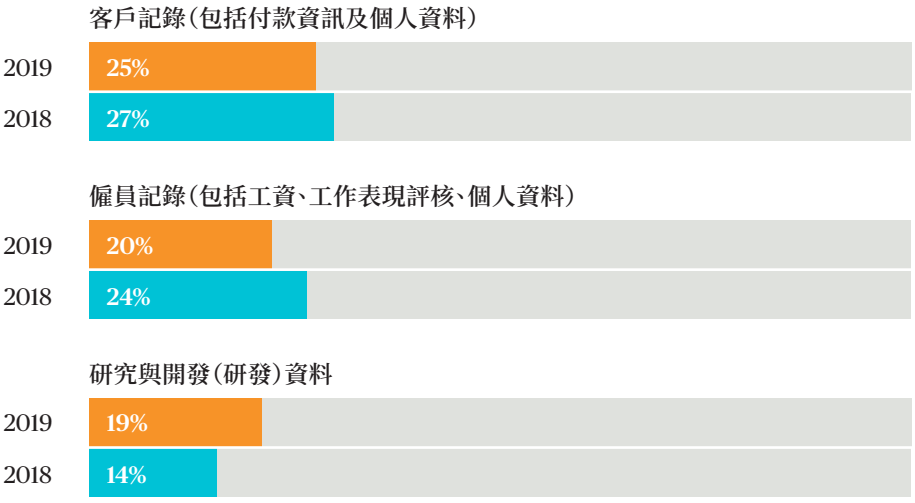
2019年的調查發現，76%的中小企業於過去12個月曾遭遇網絡事故，較2018年的71%略有上升。

最為常見的網絡事故類型為因系統或技術故障導致資料遺失(29%)，其次是人為錯誤(24%)及因系統或技術故障導致業務中斷(18%)。

令人擔憂的事實：2019年與2018年最常遭遇的網絡事故對比



最常被洩露的資料檔案與2018年類似：

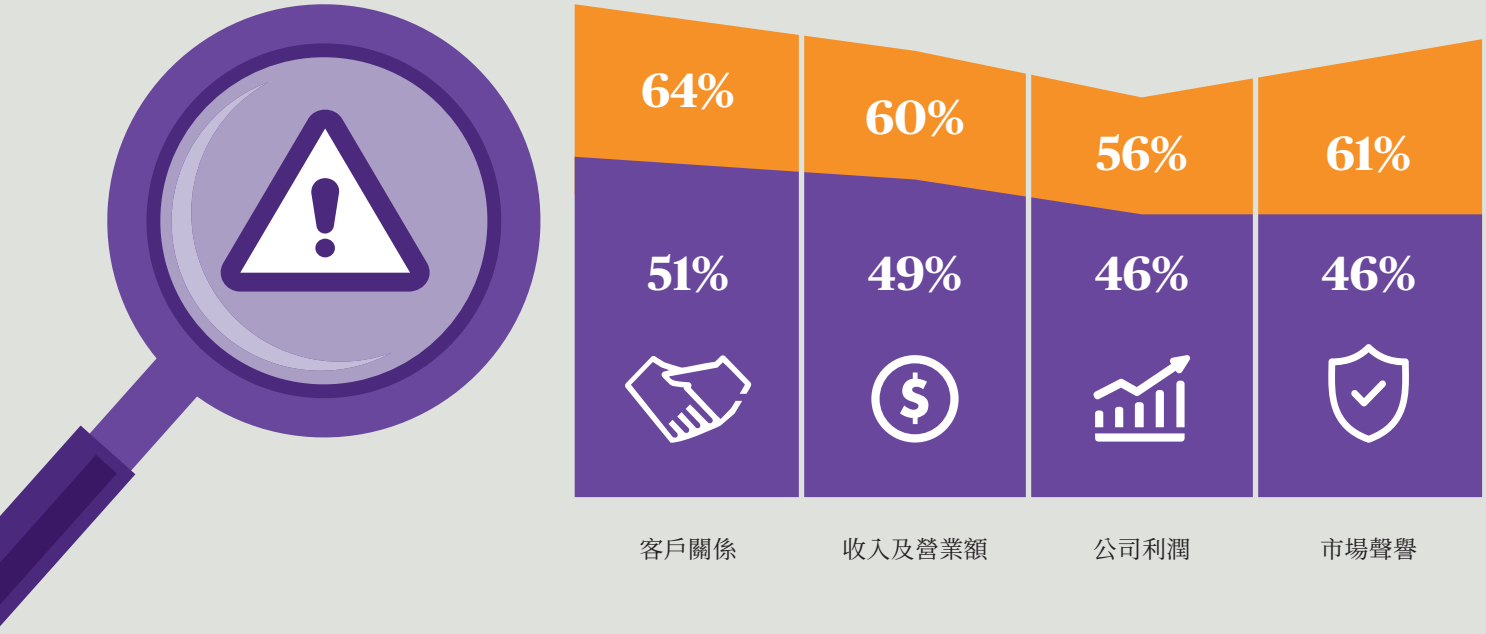


以客戶為先

調查發現，發生重大網絡事故後，中小企業最關心的是網絡事故對其與客戶關係(51%)的影響，此數字較2018年(64%)為低；其次是對收入及營業額(49%)、公司利潤(46%)及市場聲譽(46%)的影響。

儘管存在這些憂慮，但在發生網絡事故後，逾三分之一(34%)的中小企業雖然會檢討保安措施，卻並無採取進一步行動，僅有11%的企業嘗試修復遭破壞的資料檔案。

中等至嚴重程度的影響



僱員是最佳防禦

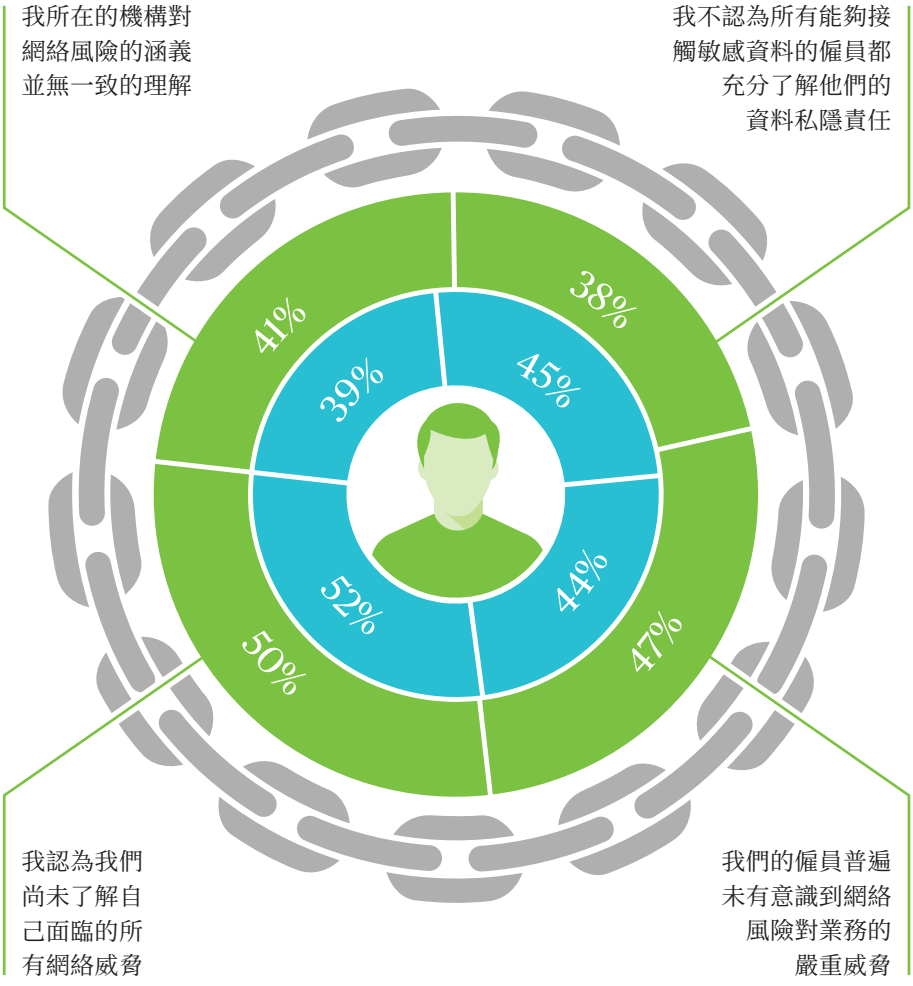
對希望提高網絡防禦水平的中小企業而言，僱員既是最大的風險，亦是最佳的防禦。作為企業的第一道防線，僱員能夠在偵測及防止資料洩露方面發揮關鍵作用。

目前，有半數(50%)香港中小企業領導者認為，僱員並不了解自己所面臨的所有網絡威脅。

近半數(47%)領導者表示，僱員並未意識到企業所面臨網絡風險的嚴重性。另有41%的領導者則表示，對於網絡風險的涵義，企業內部並無一致的理解，因此，讓僱員建立網絡風險意識最為重要。

此外，38%的中小企業領導者不認為所有能夠接觸敏感資料的僱員都充分了解他們的資料私隱責任。

僱員有否做足準備，成為公司的最佳防禦？



案例: 勒索軟件攻擊

全年收入約為：
2,740萬港元

行業：
建築

費用：
超過260萬港元

有一間將資訊科技運作外判的建築公司，由於一名僱員點擊了惡意電郵連結，遭勒索軟件攻擊，導致公司的客戶及項目資料被加密。

勒索軟件感染了本地硬碟及線上備份的資料，由於無法讀取記錄，公司無法正常經營業務。該公司與勒索者談判破裂，其後因重新構建和重新輸入客戶項目記錄而耗費額外成本，並導致長時間停工，更令業務蒙受重大損失。

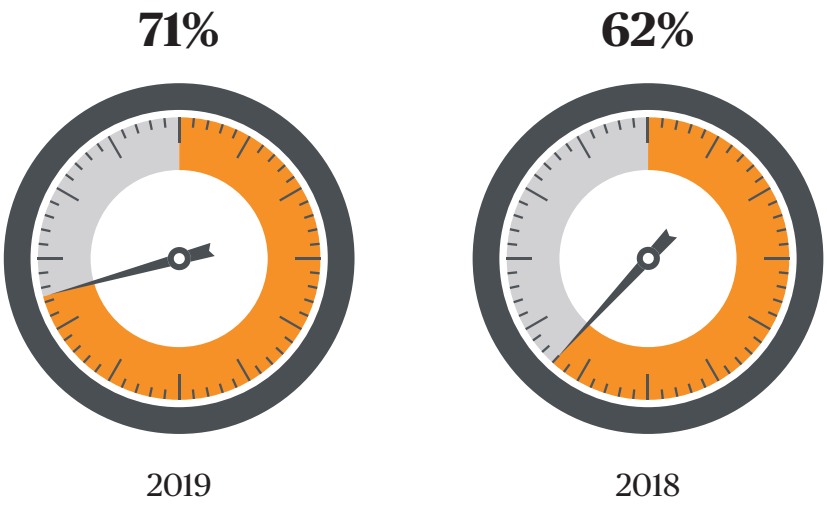
速度的必要性

相對去年，香港的中小企業應對網絡事故的速度有所改善，71%的企業能夠在網絡事故發生後12小時內恢復營運，較2018年的62%大幅增加。

超過三分之二(69%)的中小企業會在72小時內與受影響的持份者溝通，而2018年則為62%。64%的中小企業領導者表示，相關僱員已了解適當的應急計劃，一旦發生網絡事故，將按計劃執行危機應對流程，而於2018年只有56%。

人們普遍認為，應對計劃越好意味著資料外洩應急計劃越完善，但情況並非如此。雖然調查發現香港的企業在緊急應變時間方面有所改善，但仍有過半數(54%)的企業尚未制定適當的資料外洩應急計劃。

更多企業能夠在網絡事故發生後12小時內恢復營運



暗藏危機

持續性威脅可在中小企業的網絡中潛伏多年。Infocyte於2019年7月發佈的美國報告指出，潛伏時間（某種威脅在被發現並清除之前在網絡中存在的時間）已成為中小企業面臨的嚴峻問題。勒索軟件攻擊的潛伏時間平均為43天，而所有其他持續性威脅（非勒索軟件）的潛伏時間則長達798天。值得警惕的是，風險軟件（定義為垃圾應用程式、網絡跟蹤程式及廣告軟件）的潛伏時間平均長達869天。

該報告指出，72%的中小企業的網絡中存在需耗時90天以上方可清除的風險軟件和垃圾應用程式。儘管這些問題所涉風險普遍較低，但更嚴重的問題在於，倘若網絡無法控制風險軟件，當發現更高級別的威脅時，往往亦無力應對。

該報告建議，即使無法進行持續監控，中小企業至少亦應委聘第三方進行資料外洩評估。

保險的重要角色

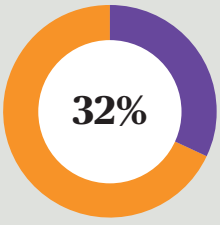
今年的研究表明，越來越多的中小企業開始了解網絡風險的嚴重性。68%的中小企業表示已從過往的網絡事故中汲取教訓，未來發生此類事件的可能性較小，而於2018年此比例為59%。

發生網絡事故後，香港59%的中小企業領導者亦會加強資料文檔的保安並改善處理資料的流程，而2018年則為46%。

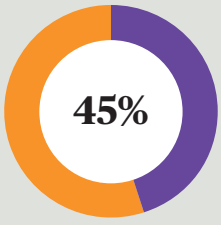
顯然，香港中小企業的網絡風險意識日漸加強，但仍普遍缺乏主動保護措施。將近三分之一(32%)的中小企業在遭遇網絡攻擊前後並無購買網絡保險。雖然這一比例較2018年的53%大幅下降，但仍有近半數(45%)的中小企業尚未全面了解市面上的保險方案以及保險對於網絡風險管理的作用。發生網絡事故後，中小企業最重視監管建議(60%)，其次是緊急應變速度(57%)及能否獲取緊急應變服務(57%)。

中小企業是否已投保網絡保險	2019	2018
是 — 我們目前已投保該保險	33%	26%
是 — 我們曾投保該保險，但保障已失效	16%	20%
否 — 我們從未投保此類保險	47%	48%
不知道	4%	7%

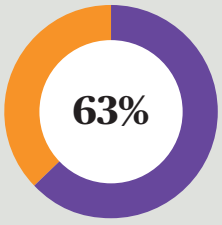
發生網絡事故後採取的行動



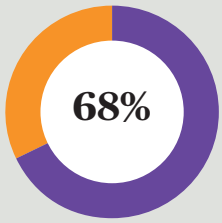
32%的中小企業在遭遇網絡攻擊前後均無購買網絡保險。



45%的中小企業尚未全面了解市面上的保險方案以及保險對於網絡風險管理的作用。



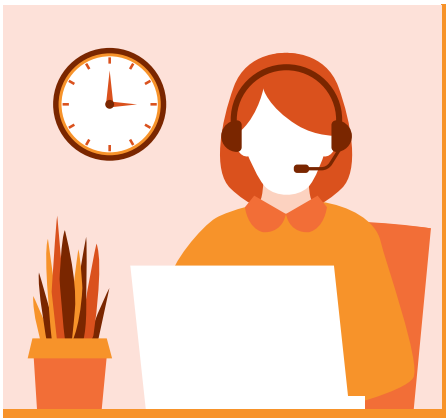
63%（於2018年的比例為46%）的中小企業領導者亦會加強資料文檔的保安並改善處理資料的流程。



68%（於2018年的比例為59%）的受訪者表示已從過往的網絡事故中汲取教訓，未來發生此類事件的可能性較小。

減輕損失的服務

安達保險的所有中小企業網絡保險客戶均可享受重要的減輕損失服務，包括：



緊急應變平台

安達保險為客戶提供緊急應變平台，以控制事故威脅及潛在損害。平台的服務包括跟據第三方合約的服務承諾，提供全年24小時危機應對熱線，服務承諾要求事故經理於一小時內回覆，並籌組專家團隊協助管理和紓緩一系列的網絡風險，包括拒絕服務攻擊、勒索軟件、網絡罪行及僱員失誤，以及事後報告。過往12個月，安達保險對亞太區客戶的網絡事故初步回覆時間平均為12分鐘。

網絡釣魚評估

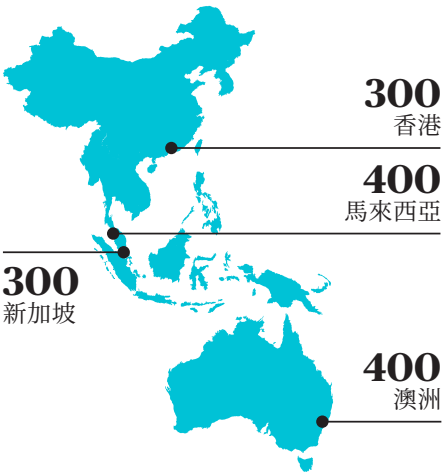
安達保險與網絡釣魚研究專家合作，提供網絡釣魚意識評估。評估內容包括兩個模擬的現實網絡釣魚場景，在四個月內可針對多達500個獨立電郵地址進行測試。

免費的密碼管理

要記住多個密碼頗為困難。企業可選擇採用一體化解決方案，儲存並自動填寫用戶密碼及登錄資料。借助安全共享功能，同事之間甚至毋須得知彼此的密碼即可共享登錄。更可採用暗網監控功能掃描網絡，一旦發現用戶的個人資料在線上被挪作他用，便會即時提醒用戶。

關於本調查

本報告綜合了四個地區共1,400家中小企業受訪者調查的結果；包括澳洲及馬來西亞各400家，以及香港及新加坡各300家。



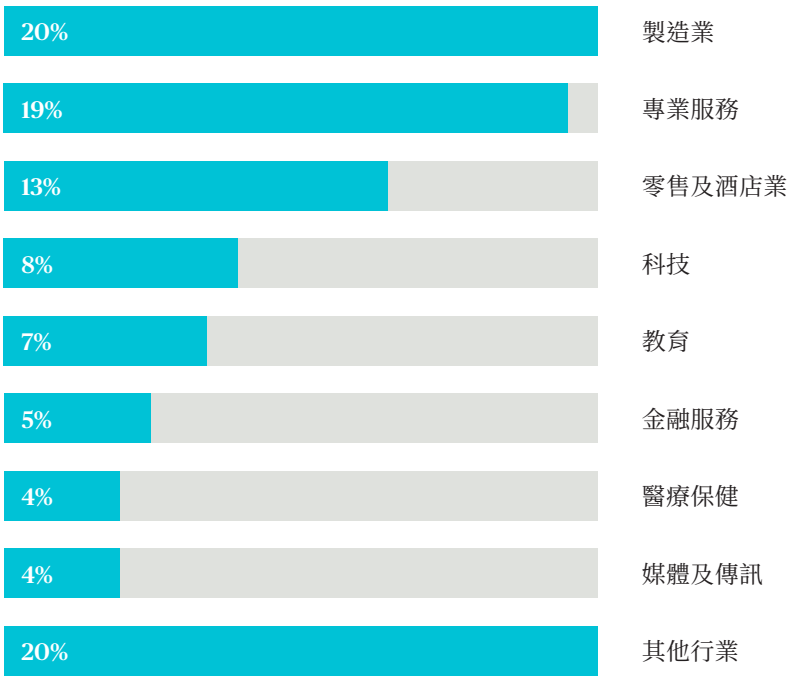
受訪者包括：

82%
董事級的高級行政人員

18%
高級經理或董事級以下的總監

來自僱員人數介乎2至249人的中小企業

受訪者所屬行業為：



中小企業可用於保障其業務的實用措施：

制定並落實密碼政策 — 強制要求僱員設定複雜難記的密碼，或許有點不近人情，但卻十分必要。建議採用複雜的密碼（字母、數字與符號的組合）並定期更改。一旦僱員離職，應立即取消其存取權限。

制定網絡事故應變計劃 — 37%的香港中小企業承認，其現有計劃僅為臨時性質，並無明文記錄。現已制定計劃的中小企業當中，僅有47%定期對計劃進行測試。我們建議企業在網絡專家的協助下制定網絡事故應變計劃，並定期對計劃進行模擬測試。

定期為僱員開展網絡安全意識培訓 — 只要一點擊惡意連結，便可能讓整個企業遭受網絡釣魚或勒索軟件攻擊。同樣，輕信「資訊科技支援」等來電，亦可能讓網絡罪犯成功竊取密碼。

更新資訊科技設備並安裝安全防護軟件 — 未安裝安全補丁的機器更易受到遠程操控，倘若僱員擁有不必要的高級管理權限，則風險更高。

關於安達香港

安達為全球最大的上市財產及責任保險公司，經營一般保險及人壽保險業務，透過收購其前身公司，已立足香港特別行政區超過90年。安達香港的一般保險業務 (安達保險香港有限公司) 為大型及中小企業客戶、以及個人客戶設計及提供特定的保險產品，包括財產險、責任險、海上險、金融險和個人保險服務。多年來，安達憑著其雄厚財務實力及市場領導地位，開創新的保險產品，提供優質服務，建立長遠穩健的客戶關係，與時並進。

如欲獲取更多資料可瀏覽
www.chubb.com/hk

聯絡資料

安達保險香港有限公司
香港鰂魚涌英皇道979號
太古坊一座39樓
電話 +852 3191 6800
傳真 +852 2560 3565
www.chubb.com/hk

Chubb. Insured.™

重要事項：